BeyondTrust

Addressing BSP's Enhanced Guidelines on Information Security Management

A BeyondTrust Guide to The Monetary Board of the Philippines' Revised Information Security Risk Management Framework

TECH BRIEF

TABLE OF CONTENTS

Introduction

In November 2017, the Monetary Board of the Philippines (the Bangko Sentral ng Pilipinas, or the 'BSP') revised its information security management guidelines to conform with the rapidly-evolving technology and cyber-threat landscape. The revised instructions published on 'Circular No. 982' contain amendments of relevant provisions of the Manual of Regulations for Banks (MORB) and the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI). These guidelines should be adopted to ensure best practices are followed organisation-wide.

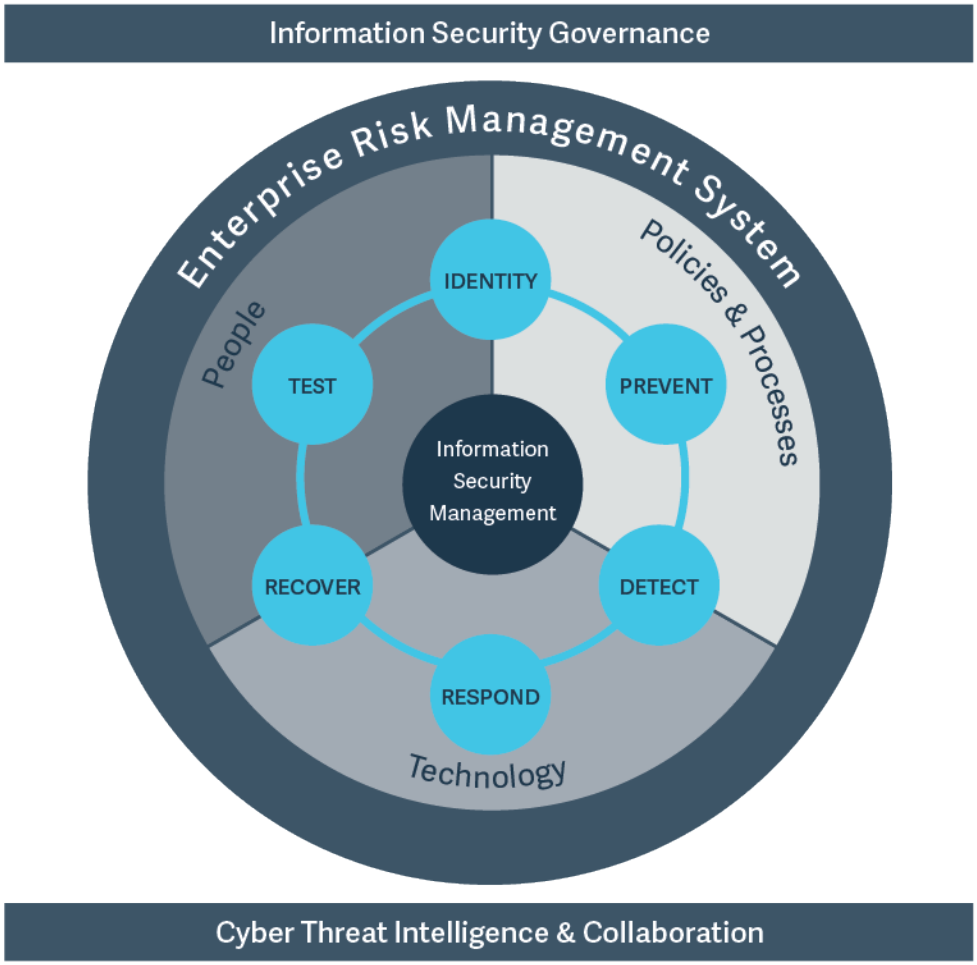
According to the BSP's "Enhanced Guidelines on Information Security Management" (Circular No. 982), all Bangko Sentral Supervised Financial Institutions (BSFIs) should establish robust and effective technology risk management processes, governance structures, and cybersecurity controls. This is to ensure that the benefits derived from technological innovations can be fully optimised without compromising financial stability, operational resilience, and consumer protection. The guidelines should also be adopted by any organisation–even outside the financial services industry—in order to protect against cyber security threats.

IT Profile Classification

BSP's first directive is to classify the IT profile of all BSFIs according to their inherent risk levels before the application of any mitigation controls. The three levels of classification* –"Complex", "Moderate", or "Simple" – are set according to six main drivers: the BSFI's IT infrastructure and operations; digital/electronic financial products and services offered; its IT projects and initiatives; outsourced services it hires; its systemic importance ("Domestic Systemically Important Bank" or not); and the volume, type, and severity of cyber-attacks and fraud targeting the organisation in question. (*Note: A general description for each IT Profile Classification is outlined in the revised guidelines. Please reference the Circular 982, page 3, for full descriptions and attributes.)

IT Risk Management System (ITRMS) & the New Information Security Risk Management Framework

The BSP's Enhanced Guidelines attest that information is a vital asset of a BSFI and must be adequately protected and managed to preserve its confidentiality, integrity, and availability. The Guidelines offer a new Information Security Risk Management (ISRM) Framework with the goal of driving a holistic, integrated, and cyclical approach to managing information security risks.



Adaptation of BSP's Information Security Risk Management Framework, Circular No. 982, Pg 6

The BSP's ISRM framework is based on four underlying fundamental principles and concepts: (1) Strong leadership and effective information security governance and oversight; (2) Integrated, holistic, and risk-based approach; (3) Continuing Cycle; (4) Cyber-threat intelligence and collaboration.

The Continuing Cycle

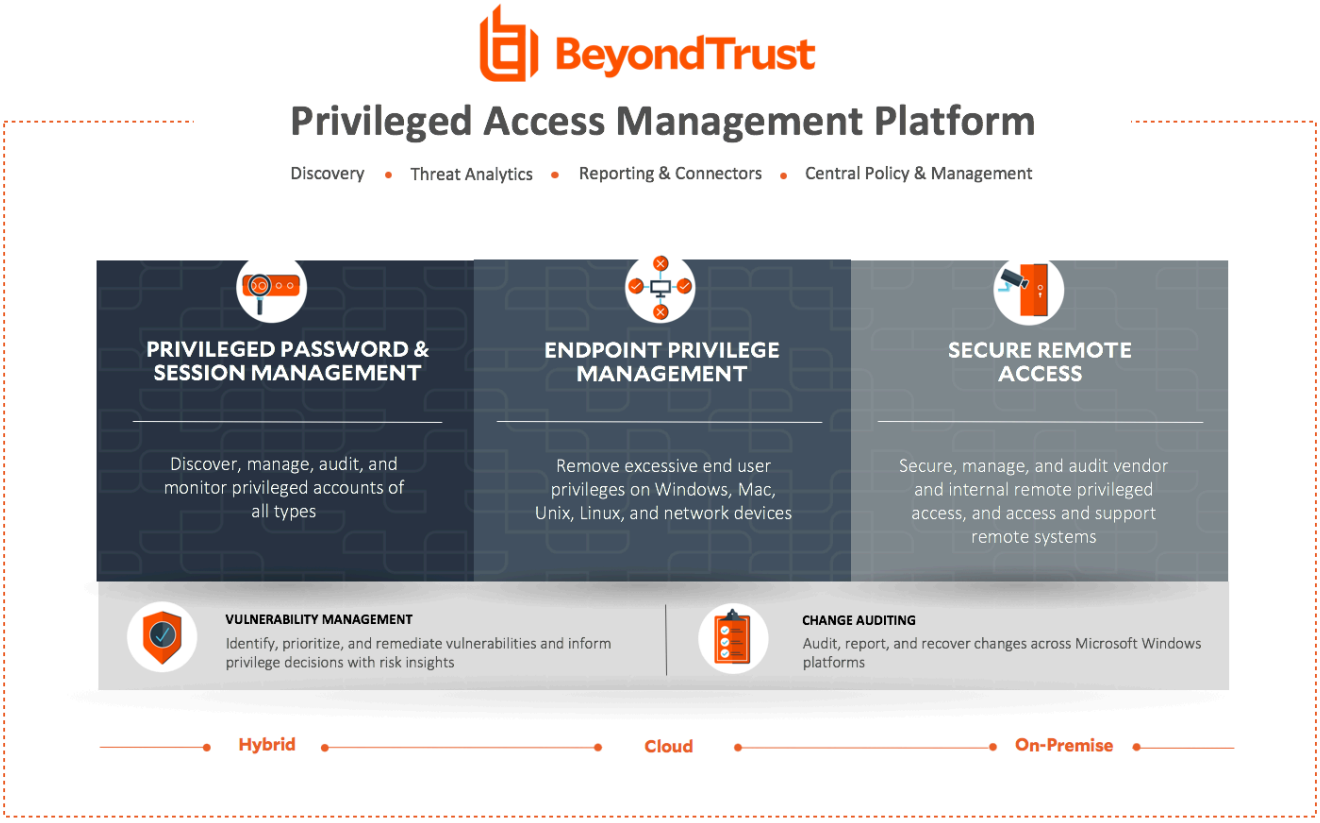
BeyondTrust can help organisations address all four principals in the BSP's ISRM Framework, especially the guidelines detailed in the "Continuing Cycle" (Principle #3). The following table maps how BeyondTrust Privileged Access Management solutions help organisations meet each directive.

Mitigation Strategies in the "Continuing Cycle"	How BeyondTrust Can Help
STEP 1 - IDENTIFY "(…) management needs to identify its business processes and functions, information assets classified as to sensitivity and criticality, threats and vulnerabilities, interconnections, and security architecture. Identification of these factors facilitates BSFI's understanding and assessment of its inherent information security and cyber risks which are key inputs in determining, designing, and implementing the appropriate risk treatment options."	BeyondTrust's Privileged Access Management (PAM) Platform enables information technology and security teams to automatically discover all privileged accounts and assets across the organisation. The solution provides a complete account and asset inventory for cyber threat management. The technology identifies high-risk users and assets by teaming behavioural analytics and vulnerability data with security intelligence from best-of-breed security solutions. In addition, BeyondTrust Vulnerability Management can uncover vulnerabilities across the network, applications, operating systems, containers, web, virtualised assets, the cloud, IoT, ICS, SCADA, and database environments.
STEP 2 - PREVENT "(…) adequate protection mechanisms and controls are designed and implemented. These include measures ranging from baseline to advanced tools and approaches such as defence-in-depth, malware prevention, access controls and cybersecurity awareness programs, among others. (…) Categorised into three types: Administrative controls, Physical and environmental controls, Technical controls."	The BeyondTrust PAM Platform is a comprehensive, integrated privileged access management platform that helps organisations reduce their attack surface by protecting what matters the most – privileged accounts with access to sensitive systems and information. The platform provides visibility and control over all privileged accounts and users, wherever they are – on the endpoint, network, on-premise, or in the cloud. The technology also provides the ability to remove administrator rights from desktops and servers and implement the concept of least privilege. By implementing least privilege, organisations ensure that users, applications, systems, and processes only have access to the tasks necessary to perform an authorised, legitimate function, and nothing further.
STEP 3 - DETECT "(…) Management should design and implement effective detection controls over the BSFI's networks, critical systems and applications, access points, and confidential information."	The BeyondTrust PAM Platform provides the capability to detect privileged access to applications, resources, and network devices that may contain sensitive information or be classified as critical infrastructure. In addition, BeyondTrust Vulnerability Management can detect changes in assets from ports, software, shares, processes, and even users that may indicate malicious intent and unauthorised changes to assets.

Mitigation Strategies in the "Continuing Cycle"	How BeyondTrust Can Help
STEP 4 - RESPOND "(…) (the BSFI) should develop comprehensive, updated, and tested incident response plans supported by well-trained incident responders, investigators, and forensic data collectors. Through adequate response capabilities, the BSFI should be able to minimise and contain the damage and impact arising from security incidents, immediately restore critical systems and services, and facilitate investigation to determine root causes."	The BeyondTrust PAM Platform offers the broadest set of privilege and vulnerability reports and connectors available in the market. IT security teams can understand and communicate risk with over 280 privilege, vulnerability, and compliance reports that can be customised to suit specific needs. With an expanding library of connectors, we make it easy to share privilege and vulnerability data with solutions for SIEM, GRC, ticketing, and many others to effectively address any developing cyber threat.
STEP 5 - RECOVER "(…) Management should be able to establish back-up facilities and recovery strategies to ensure the continuity of critical operations. (…) It should ensure that information processed using back-up facilities and alternate sites still meet acceptable levels of security. To achieve cyber resilience, the BSFI should consider information security incidents and cyber-related attack scenarios in its business continuity management and recovery processes."	BeyondTrust Auditor centralises real-time change auditing for Active Directory (AD), File Systems, Microsoft Exchange and SQL, and NetApp. The solution is capable of performing real-time backup and recovery of Active Directory objects and attributes, and allows environments to recover changes from a simple attribute to an entire OU. This recovery process documents all changes to AD and allows a selective or complete restore in case of a configuration mistake or malicious activity.
STEP 6 - TEST "The BSFI needs to continually assess and test controls and security measures implemented under the prevent, detect, respond, and recover phases to ensure that these are effective and working as intended. Likewise, a comprehensive, systematic and layered testing and assurance program covering security processes and technologies should be in place (…)."	BeyondTrust's Privileged Access Management and Vulnerability Management solutions are tightly integrated within the BeyondInsight centralised management and report console. BeyondInsight provides a single, integrated platform to continuously test, alert, and report on test controls and security measures throughout an environment. Specific parameters include privileged access, session monitoring, privileged application usage, vulnerability management, configuration compliance, and patch management.

The BeyondTrust Privileged Access Management Platform

Each of the solutions referenced to meet the requirements of the BSP's ISRM Framework are included in the **BeyondTrust Privileged Access Management Platform** – an integrated, extensible solution to provide control and visibility over all privileged accounts and users.



ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing data breaches related to stolen credentials, misused privileges, and compromised remote access.

Our extensible platform empowers organisations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. BeyondTrust unifies the industry's broadest set of privileged access capabilities with centralised management, reporting, and analytics, enabling leaders to take decisive and informed actions to defeat attackers. Our holistic platform stands out for its flexible design that simplifies integrations, enhances user productivity, and maximises IT and security investments.

BeyondTrust gives organisations the visibility and control they need to reduce risk, achieve compliance objectives, and boost operational performance. We are trusted by 20,000 customers, including half of the Fortune 500, and a global partner network. Learn more at www.beyondtrust.com

V2019_05_ENG